**INDEX**

|  |  |  |  |
| --- | --- | --- | --- |
| **Sr.No.** | **Name of experiments** | **Page Nos.** | **Signatures** |
| 1. | To detect and remove spyware, malware, viruses, worms etc. from the computer and implementing proper measures to secure it. | 2 |  |
| 2. | To use utilities like Ping, tracert, Nslookup, Netstat Nmap, Cain & Abel, Sqlmap, etc. | 4 |  |
| 3. | To use any one open source packet capture software like Wire shark to capture,  filter, inspect packets and capture passwords. | 8 |  |
| 4. | To implement IPSec using CISCO Packet Tracer. | 9 |  |
| 5. | To configure Adhoc networks. | 10 |  |
| 6. | To install and use a PTT application on Smart phones. | 13 |  |
| 7. | To Simulate a Wireless Local Area Network using CISCO Packet Tracer | 14 |  |
| 8. | To install and configure wireless access points. | 20 |  |
| 9. | To connect multiple devices using Bluetooth and PAN. | 21 |  |
| 10. | To Configure VoIP in CISCO Packet Tracer. | 22 |  |

**1.To detect and remove spyware , malware , viruses , worms etc. from the computer and implementing proper measure to secure it.**

**Malware**

Malware is one of the biggest threats to the security of your computer, tablet, phone, and other devices. Malware includes viruses, spyware, ransomware, and other unwanted software that gets secretly installed onto your device. Once malware is on your device, criminals can use it to steal your sensitive information, send you unwanted or inappropriate ads, demand payment to unscramble data encrypted by ransomware, and make your device vulnerable to even more malware. Here’s what to know to recognize, remove, and avoid malware.

**How to detect**

Look for unusual behavior from your phone, tablet, or computer.

You device might have been infected with malware if it.

* suddenly slows down, crashes, or displays repeated error messages
* won’t shut down or restart
* won’t let you remove software
* serves up lots of pop-ups, inappropriate ads, or ads that interfere with page content
* shows ads in places you typically wouldn’t see them, like government websites
* shows new and unexpected toolbars or icons in your browser or on your desktop
* uses a new default search engine, or displays new tabs or websites you didn’t open
* keeps changing your computer’s internet home page
* sends emails you didn’t write
* runs out of battery life more quickly than it should
* **How To Remove**
* **Stop shopping, banking, and doing other things online**that involve usernames, passwords, or other sensitive information — until you get your device cleared of any malware.

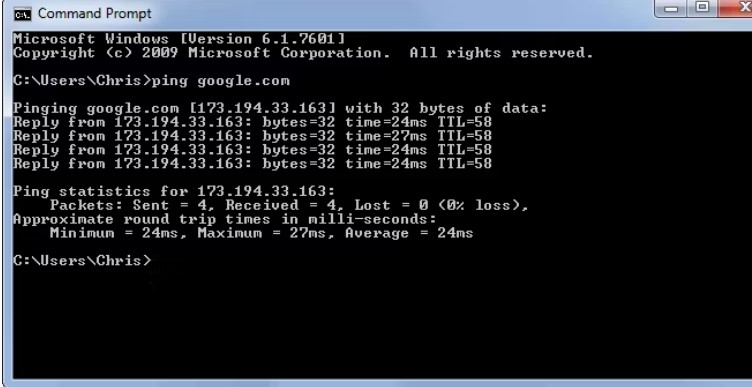
1. **Check to see if you have security software on your device — if not, download it.** Find recommendations from independent review sites by doing a search online. Some software that claims to be security software to protect you from malware *is*malware.
2. **Make sure your software is up to date.**Check that all software — the operating system, security software, apps, and more — is up to date. Consider turning on automatic updates so your software always stays up to date.
3. **Scan your device for malware**. Run a malware or security Delete anything it identifies as a problem. You may have to restart your device for the changes to take effect.
4. **Run your scan** **again to make sure everything is clear**. If the scan shows there are no more issues, you’ve likely removed the malware.
5. **Recover your operating system**. To find out how to recover your operating system (like Windows or Mac OS), visit your device manufacturer’s website. Recovering your system typically means you’ll get back a lot of the data stored on the device.
6. **Reinstall your operating system.** To find out how to reinstall your operating system (like Windows or Mac OS), visit your device manufacturer’s website. Reinstalling your system is the safest way to clean an infected device.

**2. To use utilities like ping, tracert, nslookup, netstst, nmap, chain & abel etc.**

Tools like ping, traceroute, lookup, whois, finger, netstat, ipconfig, and port scanners are available on nearly every operating system you can get your hands on. They're used for everything from troubleshooting a connection to looking up information. Whether you're using Windows, Linux, or Mac OS X, these tools are always close at hand. You'll also find web-based versions of many of these utilities. Some are even available in [Chrome OS's hidden Crosh shell](https://www.howtogeek.com/170648/10-commands-included-in-chrome-oss-hidden-crosh-shell/).

**Ping**

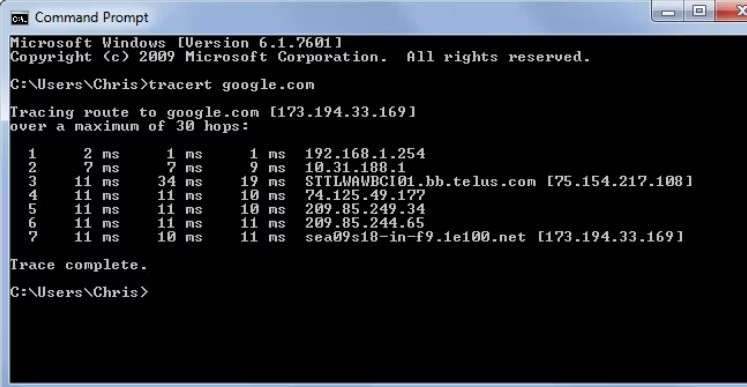
The ping command sends ICMP echo request packets to a destination. For example, you could run **ping google.com** or **ping 173.194.33.174** to ping a domain name or IP address. These packets ask the remote destination to reply. If the remote destination is configured to reply, it will respond with packets of its own. This tool can help you [troubleshoot Internet connection problems](https://www.howtogeek.com/126265/how-to-troubleshoot-internet-connection-problems/), but bear in mind that many servers and devices are configured not to reply to pings.

****

**traceroute / tracert / tracepath**

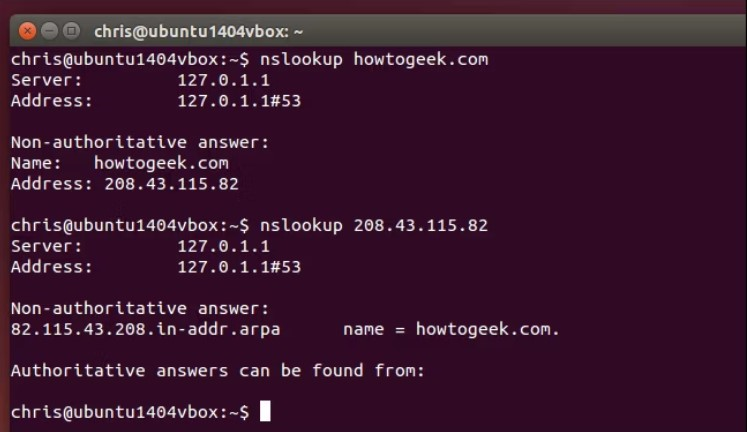
This command is similar to ping, but provides information about the path a packet takes. traceroute sends packets to a destination, asking each Internet router along the way to reply when it passes on the packet.

This will show you the path packets take when you send them between your location and a destination.This tool can help troubleshoot connection problems. For example, if you can't communicate with a server, running [traceroute may show you where the problem is occurring](https://www.howtogeek.com/134132/how-to-use-traceroute-to-identify-network-problems/) between your computer and the remote host.

****

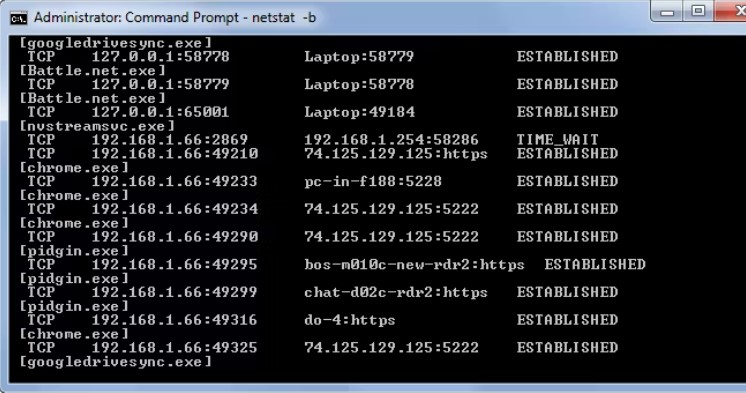
## Nslookup

## nslookup command will look up the IP addresses associated with a domain name. For example, you can run ****nslookup howtogeek.com**** to see the IP address of How-To Geek's server. This command just allows you to do it manually.nslookup also allows you to perform a reverse lookup to find the domain name associated with an IP address. For example, ****nslookup 208.43.115.82**** will show you that this IP address is associated with howtogeek.com.

****

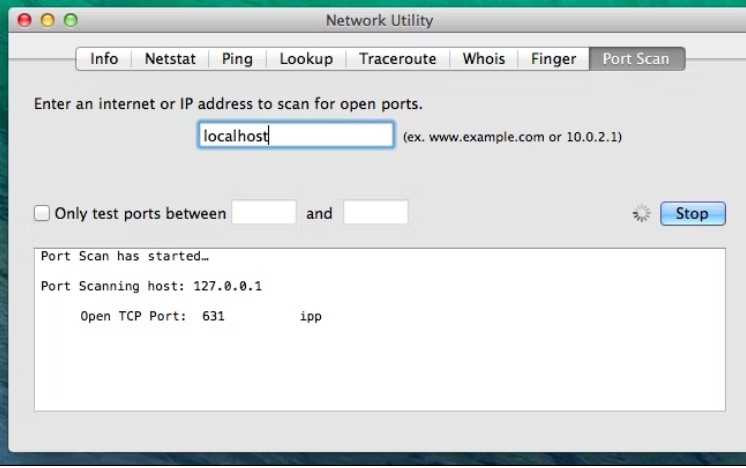
## Netstat

## netstat stands for network statistics. This command displays incoming and outgoing network connections as well as other network information. It's available on Windows, Mac, and Linux each version has its own command-line options you can tweak to see different types of information. The netstat utility can show you the open connections on your computer, which programs are making which connections, how much data is being transmitted, and other information.



## Port Scan / nmap

The nmap utility is a common tool used for port scans, but there are many utilities that can run this sort of scan. A port scan is the process of attempting to connect to every port on a computer -- ports 1 through 65535 -- and seeing if they're open. An attacker might port-scan a system to find vulnerable services. Or, you might port scan your own computer to ensure that there are no vulnerable services listening to the network.



[**Nmap**](https://www.networkworld.com/article/966196/what-is-nmap-why-you-need-this-network-mapper.html)

This month marks the 20th anniversary of [Nmap](https://www.networkworld.com/article/966196/what-is-nmap-why-you-need-this-network-mapper.html), the open-source network mapping tool that became the standard used by many IT professionals, but that can be a bit much if you only need to do general network maintenance and are intimidated by its command-line interface.There are alternatives – not many – that range in technical sophistication from tools with GUIs that can ease you into performing the essentials of network maintenance to more advanced software that is similar to Nmap itself.

**Cain & Abel**

Cain & Abel is a password recovery tool for Microsoft Operating Systems. It allows easy recovery of various kinds of passwords by sniffing the network, [cracking encrypted passwords](https://www.infosecinstitute.com/skills/courses/cracking-passwords/?utm_source=resources&utm_medium=infosec+network&utm_campaign=cracking+passwords+tag&utm_content=sidebar+top) using Dictionary, Brute-Force and Cryptanalysis attacks, recording VoIP conversations, decoding scrambled passwords, recovering wireless network keys, revealing password boxes, uncovering cached passwords and analyzing routing protocols.The latest version is faster and contains a lot of new features like APR (ARP Poison Routing) which enables sniffing on switched LANs and Man-in-the-Middle attacks. The sniffer in this version can also analyze encrypted protocols such as SSH-1 and HTTPS and contains filters to capture credentials from a wide range of [authentication](https://www.infosecinstitute.com/skills/courses/authentication-and-authorization/?utm_source=resources&utm_medium=infosec+network&utm_campaign=skills+pricing&utm_content=hyperlink) mechanisms.

**3. To use any open sourse packet capture software like wire shark to capture filter,inspect packet and capture password**

Few tools are as useful to the IT professional as Wireshark, the go-to network packet capture tool. Wireshark will help you capture network packets and display them at a granular level. Once these packets are broken down, you can use them for real-time or offline analysis

Wireshark is a network protocol analyzer, or an application that captures packets from

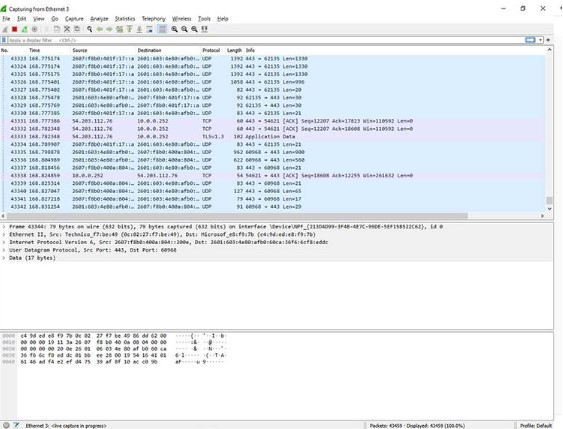
a network connection, such as from your computer to your home office or the internet.

Packet is the name given to a discrete unit of data in a typical Ethernet network.

Wireshark is the most often-used packet sniffer in the world. Like any other packet

sniffer, Wireshark does three things:

1. **Packet Capture:** Wireshark listens to a network connection in real time and then grabs entire streams of traffic – quite possibly tens of thousands of packets at a time.
2. **Filtering:** Wireshark is capable of slicing and dicing all of this random live data using filters.
3. **Visualization:** Wireshark, like any good packet sniffer, allows you to dive right into the very middle of a network packet. It also allows you to visualize entire conversations and network streams.



Packet sniffing can be compared to spelunking – going inside a cave and hiking around. Folks who use Wireshark on a network are kind of like those who use flashlights to see what cool things they can find.

**4. To implement IPSec using CISCO Packet Tracer.**

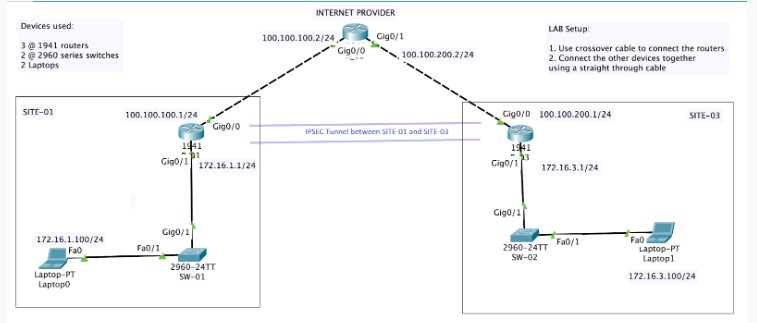
Cisco Packet Tracer allows IPSEC VPN configuration between routers. The example below presents a basic VPN configuration over a Frame Relay between Paris and New-York using Cisco 2811 routers.  
IPSEC Tunneling allows network adminisrators to use the Internet to create secure connections between networks (teleworkers, remote sites, ...). Cisco 2811 routers use the ISAKMP and IPsec tunneling standards to crete and manage tunnels. IPsec provides authentication (AH) and encryption (ESP) services to prevent unauthorized data access or modification.

**A major problem** with IPSec sessions is that they do not support multicast or broadcast traffic.   
**Solution** : Build another generic tunnel over IPSEC. Three options available in Cisco routers :

* Virtual Tunnel Interface (VTI)
* Generic Routing Encapsulation (GRE)
* DMVPN and GET VPN

This week was a rather intense one. I offered to be a volunteer trainer for a Network Security Bootcamp whose aim was to provide practical experience to new graduates and prepare them for a job in the Network Security field It has been more than 6 years since I used it so I was a little rusty, but I always say that once you properly understand networking, it’s really difficult to unlearn it. This blog is a summary of the hand-on lab that I prepared for the students. Hope someone will find it helpful.

Below is the topology that was used for this lab and steps taken by the students.



**5. To configure ADHOC network .**

While it is not typically known by non-technical people, it is possible to connect Wi-Fi computers together without the use of a wireless router or access point; this feature is called Ad-Hoc networking.

With Ad-Hoc networking, the multiple computers are connected directly to each other through the same wireless cards used to connect to the more standard wireless router or access point. In this article we'll review the process of setting up an Ad-Hoc network .

**1.**The first step in the process requires that we start at the Network and Sharing center as shown in Figure 1 below. You can access the Windows 7 Networking and Sharing Center through your control panel.

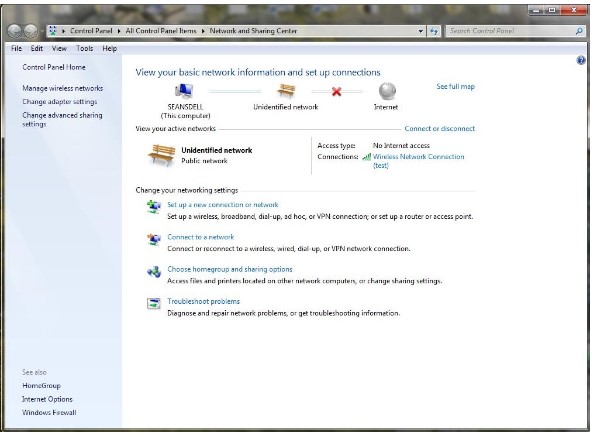


Figure 1: Windows 7 Networking and Sharing Center

Now, from this point, there are two different ways to setup an Ad-Hoc network:

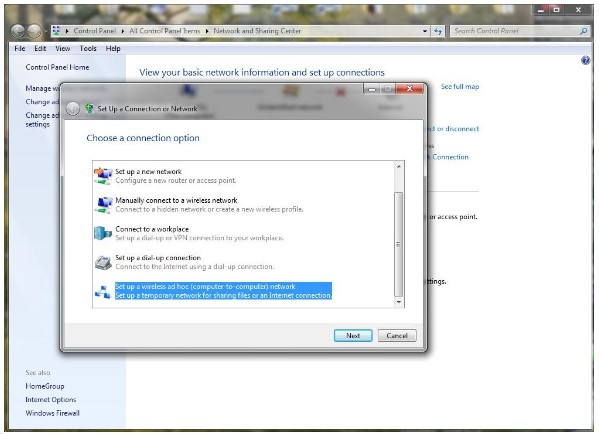
* one uses the Setup a connection or network wizard
* the other utilizes the Manage Wireless Networks control panel

The choice of which one to use depends on your preference. The setup of the Ad-Hoc network only needs to be performed on the first computer being configured.

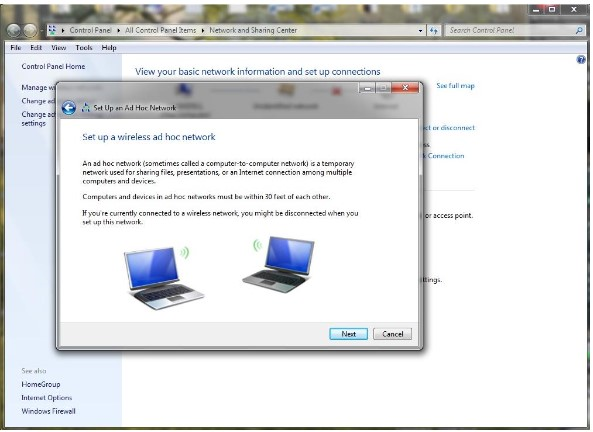
Let's review the steps using both of the setup methods.

### Ad-Hoc Network Configuration using the Setup a Connection or Network Wizard

When using the wizard method, the first task to perform requires the selection of 'Setup a new connection or network' option from the main window; this is shown in Figure 1.

Figure 2: Setup a Connection or Network

At the bottom of the list shown in the window is the option to **Set up a wireless ad hoc (computer-to-computer) network**. Once this option is selected the window shown in Figure 3 is displayed.



The window shown in Figure 3 describes the Ad Hoc network and describes the requirements. Once you review the text on this window select next.Figure 4: Give your network a name and choose security options

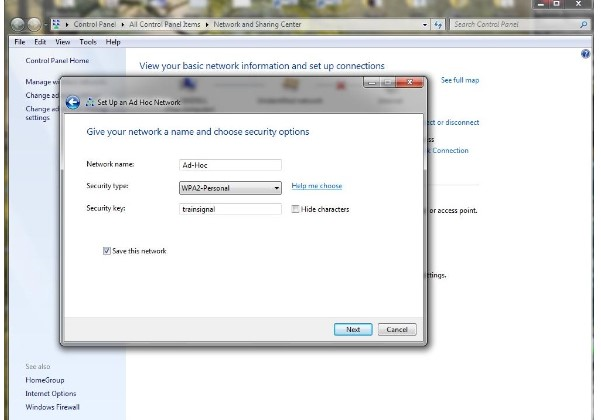
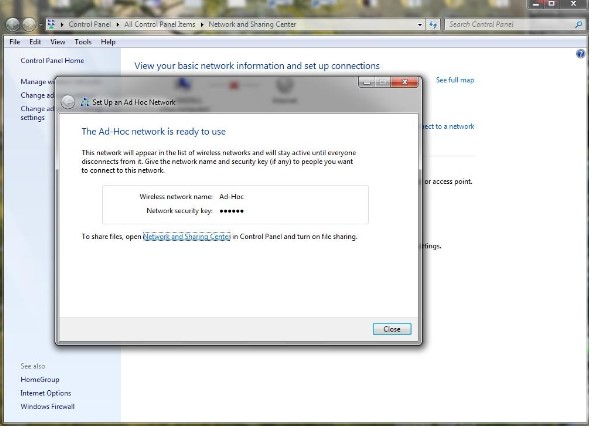


Figure 5: The Ad-Hoc network is ready to us



This completes the process using the wizard method.

**6. To install And use a PTT Application on smart phones.**

PTT Express solutions include: • PTT VoWLAN is a single mode solution designed to provide service to mobile users inside the enterprise without regard to their location inside the facility The solution provides mobile access over the enterprise Wireless Local Area Network (WLAN) to comprehensive voice and data services. This includes services such as email, and text messaging that are typically tethered to the desk.

The PTT Express client allows supported devices to create Push-To-Talk communication capability between different types of devices. Refer to the PTT Express User Guide for a list of supported devices. Some of the devices listed may require a software download/install to add PTT Express to the device, but for many of the devices PTT Express comes pre-installed.

**Installing on an Android Device Using the USB Connection :**

1. Connect the device to a host computer using the Rugged Charge/USB cable.

2. On the device, pull down the Notification panel and touch Charging this device via USB. By default, No data transfer is selected.

3. Touch File Transfer.

4. On the host computer, open a file explorer application.

5. On the host computer, copy the application APK file from the host computer to the device.

6. Disconnect the device from the host computer.

. Swipe the screen up and select to view files on the Internal Storage.

8. Locate the application APK file.

9. Touch the application file.

10. Touch Continue to install the app or Cancel to stop the installation.

11. To confirm installation and accept what the application affects, touch Install otherwise touch Cancel.

12. Touch Open to open the application or Done to exit the installation process.

13. The application appears in the App list.

**7. To stimulate a wireless local area network using CISCO Packet Tracer.**

WLAN stands for Wireless Local Area Network. WLAN is a local area network that uses radio communication to provide mobility to the network users while maintaining the connectivity to the wired network.

**Steps to Configure WLAN in Cisco Packet Tracer:**

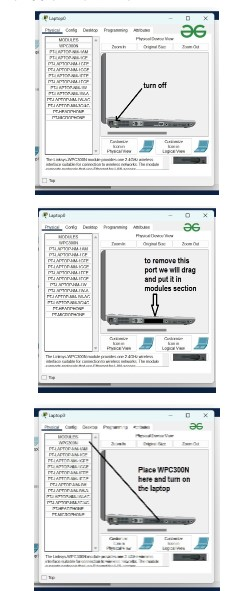
**Step1:** we need these devices to set up the network topology as shown in the table below:



By using these devices we’ll have to create a network like shown in the representation:



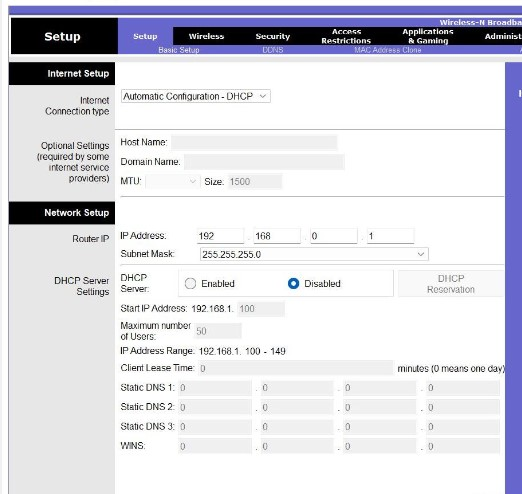
**Step 2:** Configuring laptops to make them wireless. First, click on the laptop0 and turn off its power to change the ports basically we are going to replace the wired port with the wireless port which is **WPC300N**.



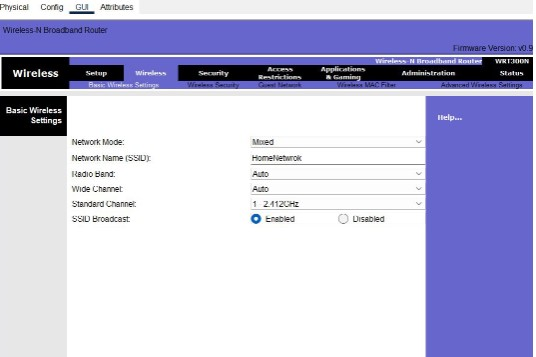
* Replace with **WPC300N** and make sure to turn it ON.
* Repeat the same procedure with **Laptop1** and**Laptop 2.**
* after that, we will assign IP addresses and a*default gateway* to the *laptops*.

**Step 3:** Configure the Router with an IP address and Generate a Security key.

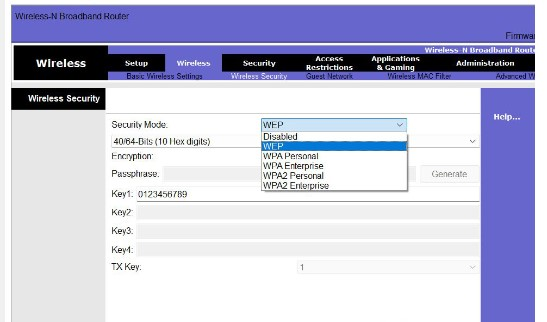
* First, click on Router and Go to GUI.
* Then click on a setup where you will find the IP address assigned to**192.168.0.1** and subnet mask**[255.255.255.0]**.
* Then disable the DHCP server because we have to configure statically.
* Then Save the **settings.**



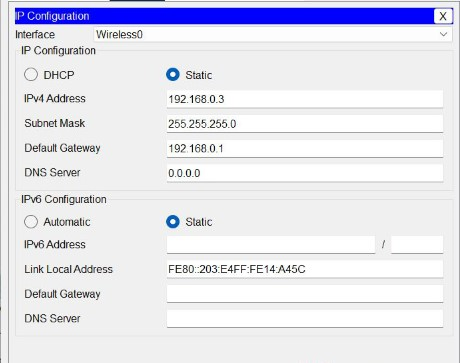
* Then move to the wireless option.
* set Network Name(SSID) is **HomeNetwork.**
* Save the **settings.**



* Then we set the security key.
* Click on **wireless security** and select security mode as **WEP**.
* Then we’ll generate KEY by entering 10 digit Hexa-numeric value. eg**: 0123456789.**
* save the settings.



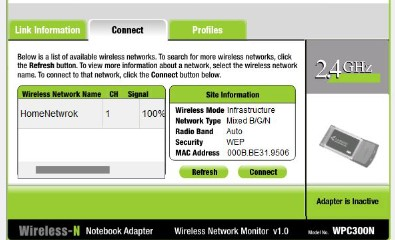
**Step 4:** Now we will configure the laptops using the IP addressing table given below:



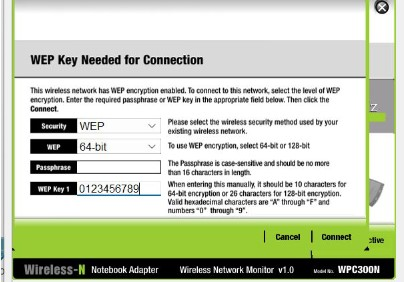
**Configure Laptop0:**To configure the laptop first set the IP configuration as static then add the IPv4 address and default gateway.

**Step 5:** Connect the laptop to the router by entering the security key in the laptop.

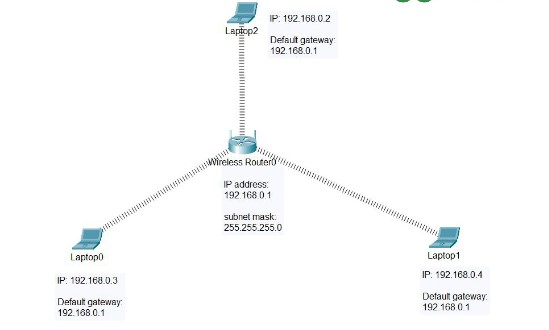
* Click on **laptop0** and go to desktop.
* Click on connect and refresh the network.
* After a few seconds, it will show the name of the network we have assigned.
* Click on HomeNetwork.



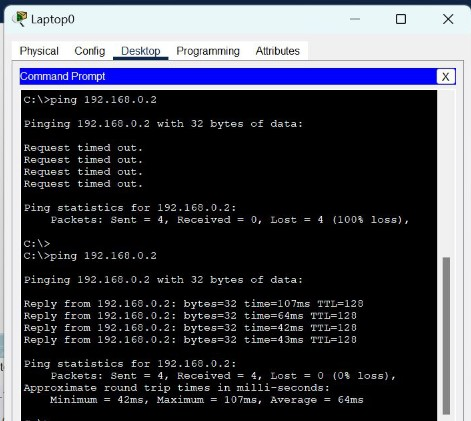
* Then enter the security key in WEP key 1 and hit on connect.
* laptop0 will connect with the router.
* Repeat the same process with Laptop1 and laptop2 so that they can connect with the router.



* After all of this, all of the hosts will connect with the router



**Step 6:** Then we’ll verify the wireless connection by pinging the IP address of any laptop or by sending and receiving data packets. For example: Go to the command prompt of Laptop0 and type the following command:



**8. To install and configure wireless access point.**

Wireless access point installation isn’t difficult but if you get it wrong, you will feel the pain. We’ve seen some really funky installations. We have heard horror stories from clients about so called “tips” that they received from self-proclaimed wireless service experts.

Our clients have told us that other providers recommended mounting access points at 45 degree angles. Or waiting up to 7 days for wireless signals to propagate within their office. Knowing that people have paid other service providers for such terrible advice is simply horrifying. We’re here to tell you the truth. Part 1 of our tips for installing wireless access points will focus on 3 key aspects:

* network requirements
* existing network environment
* physical installation.

**Part 2 will focus on:**

* advanced network configuration
* how to prime your wireless access points for peak performance.

Whether you’re [installing access points at a large office](https://www.madebywifi.com/services/office-wifi/), home, [warehouse](https://www.madebywifi.com/services/warehouse-wifi/) or open area like a park or boardwalk, taking the following steps will typically leave you with a usable WiFi network that will stay connected and provide that bandwidth throughput that you expect.

### 7 Tips for Your Wireless Access Point Installation:

### 1. Understand all of your network requirements

### 2. Choose the right equipment for your wireless network

### 3. Be aware of the network limitations of your devices

### 4. Consider the various types of cables you will need to use

### 5. Be aware of nearby interference that can impact your wireless access point installation

### 6. Select a proper location for your wireless access point

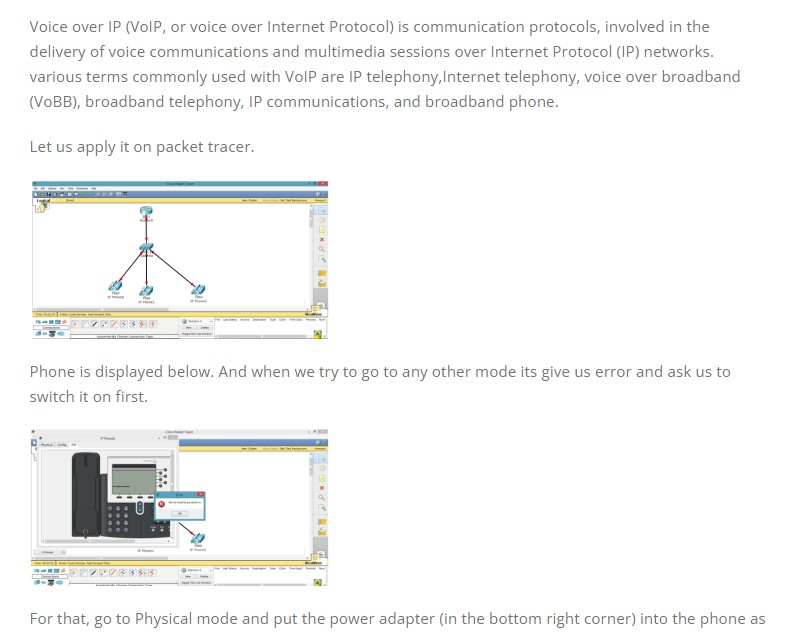
### 7. Measure signal strength before making final access point placements

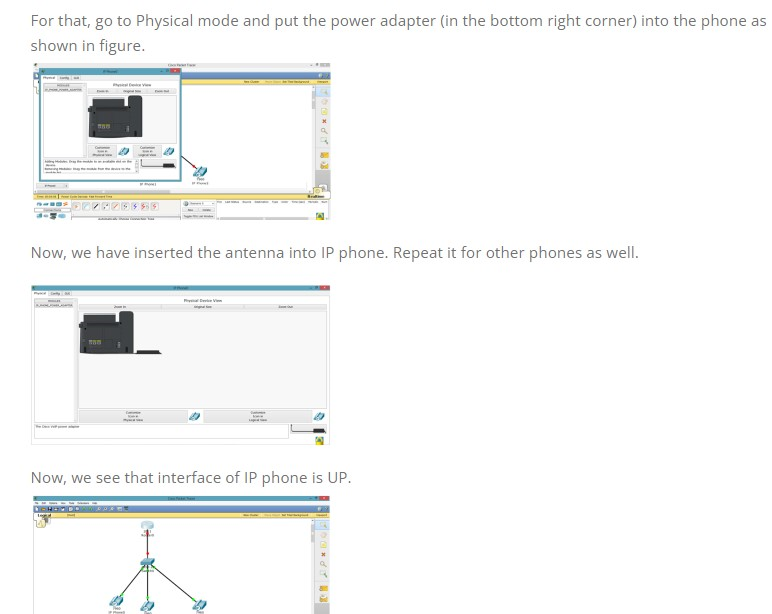
|  |  |
| --- | --- |
| **9. To connect multiple devices using bluetooth and PAN.**  After both devices have been paired, you are ready to start a direct connection between both computers. On the Laptop, right click Bluetooth taskbar icon, then click "Join a Personal Area Network" to open Bluetooth Personal Area Network Devices window. You can also get to the window via Network Connections folder by right-clicking Bluetooth Network Connection and selecting View Bluetooth Network Devices.  Join a Personal Area Network from Bluetooth taskbar icon   Bluetooth Personal Area Network Devices: connect to an ad hoc network (PAN)  **Connecting to the Desktop using PAN service via Bluetooth taskbar icon.**   |  | | --- | |  |   On Bluetooth Personal Area Network Devices window, you will find the paired computer under Direct Connections. Select Desktop and click Connect. Wait for a few seconds when you see a "Connecting..." message popping up. After that, the wireless PAN (PANU-to-PANU) is active and the Laptop is connected to the Desktop. |

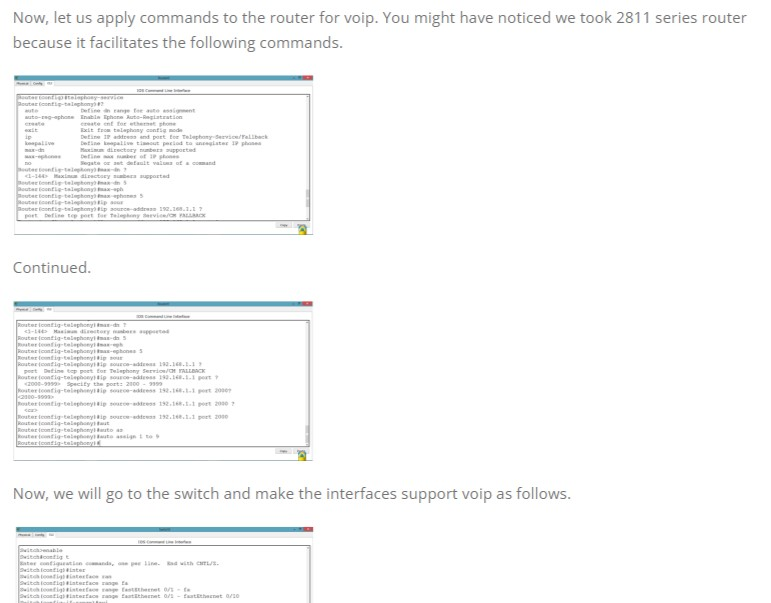
|  |  |
| --- | --- |
|  |  |

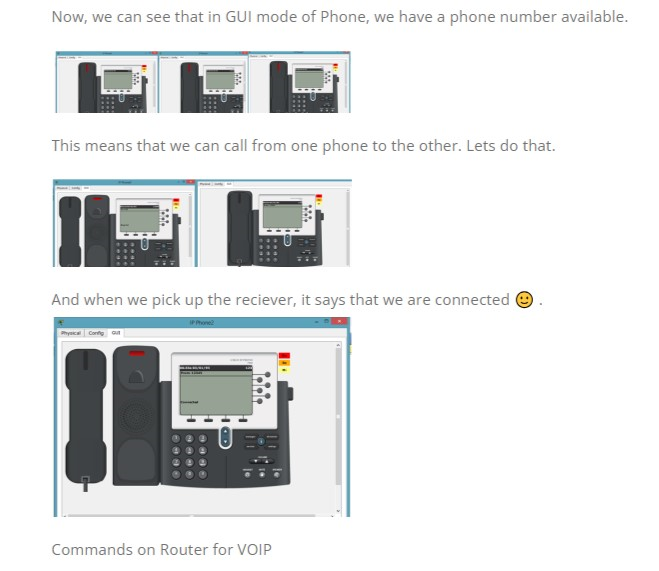
**10. To configure volp in CISCO packet tracer**

After both devices have been paired, you are ready to start a direct connection between both computers. On the Laptop, right click Bluetooth taskbar icon, then click "Join a Personal Area Network" to open Bluetooth Personal Area Network Devices window. You can also get to the window via Network Connections folder by right-clicking Bluetooth Network Connection and selecting View Bluetooth Network Devices.

****

****





**THANK YOU**